

UNITED STATES DISTRICT COURT
for the
Eastern District of Wisconsin

In the Matter of the Search of:

A silver cased iPhone, Model MQ3X2LL/A, Serial Number
F17VPX1DHYFK, IMEI 35 578907 295887 8, Device B.
Device B is currently located at North Central HIDTA and is
currently listed under Milwaukee Police Department
Inventory # 18001180 as item number 2

) Case No. 18-M-1226

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim P. 41(c) is:

- evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- property designed for use, intended for use, or used in committing a crime;
- a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: Title 18, U.S.C. Section 1965; Title 21 U.S.C. Sections 841(a)(1), (b)(1)(B) and (b)(1)(C), Title 18 U.S.C. Section 924(c)

The application is based on these facts: See attached affidavit.

Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

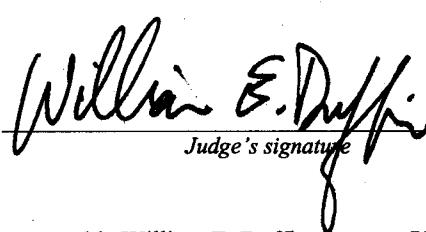


Applicant's signature

Special Agent Richard Connors, ATF
Printed Name and Title

Sworn to before me and signed in my presence:

Date: 1/25/18



Judge's signature

City and State: Milwaukee, Wisconsin

Honorable William E. Duffin, U.S. Magistrate Judge

Case 2:18-mj-01226-WED Filed 02/06/18 Page 1 of 14 Document 1

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Richard Connors, being first duly sworn, hereby depose and state as follows:

AGENT BACKGROUND AND INFORMATION

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic devices—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am employed as a Special Agent with the United States Department of Justice, Bureau of Alcohol, Tobacco, Firearms and Explosives (“ATF”) assigned to the Milwaukee Field Office since October of 2015. I have been employed as a full time law enforcement officer for over 30 months. I have received training at the Federal Law Enforcement Training Center in Glynco, GA. I attended the Criminal Investigator Training Program, as well as ATF’s Special Agent Training Program. I have received training in the investigation of unlawful possession of firearms, the unlawful transfer of firearms, and the unlawful dealing in firearms without a dealers’ license. Prior to becoming a Special Agent with the ATF, I received two (2) bachelor’s degrees from Northern Illinois University in the fields of Sociology and International Relations. I have received a Master’s degree from Northern Illinois University in the field of American Government.

3. I have received training in the investigation of firearm and drug trafficking. Based on my training, experience, and participation in firearm trafficking investigations, I know and/or have observed the following:

a. I have utilized informants to investigate firearm and drug trafficking. Through informant interviews and debriefings of individuals involved in those offenses, I have

learned about the manner in which individuals and organizations distribute these items in Wisconsin and elsewhere;

- b. I have also relied on informants to obtain firearms (as opposed to licensed gun dealers) and controlled substances from individuals on the streets, known as a controlled purchase;
- c. I have experience conducting street surveillance of individuals engaged in firearm and drug trafficking. I have participated in the execution of numerous search warrants where drugs, firearms, ammunition, and magazines have been seized;
- d. I am familiar with the language utilized over the telephone to discuss firearm and drug trafficking, and know that the language is often limited, guarded, and coded;
- e. I know that firearm and drug traffickers often use electronic equipment to conduct these operations;
- f. I know that drug traffickers commonly have in their possession, and at their residences and other locations where they exercise dominion and control, firearms, ammunition, and records or receipts pertaining to such;
- g. I know that firearm and drug traffickers often put their telephones in nominee names to distance themselves from telephones that are utilized to facilitate these and related offenses; and
- h. I know that firearm and drug traffickers often use proceeds to purchase assets such as vehicles, property, jewelry, and narcotics. I also know that firearm and drug traffickers often use nominees to purchase and/or title these assets to avoid scrutiny from law enforcement officials. I also know what firearm and drug traffickers may keep photographs of these items on electronic devices.

4. I have participated in multiple firearm and drug trafficking investigations that involved the seizure of computers, cellular phones, cameras, and other digital storage devices, and the subsequent analysis of electronic data stored within these computers, cellular phones, cameras, and other digital storage devices. In many occasions, this electronic data has provided evidence of the crimes being investigated and corroborated information already known or suspected by law enforcement.

5. This affidavit is based upon my personal knowledge and upon information reported to me by other federal and local law enforcement officers during the course of their official duties, all of whom I believe to be truthful and reliable.

6. Because this affidavit is submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only facts that I believe are sufficient to establish probable cause.

I. IDENTIFICATION OF THE DEVICES TO BE EXAMINED

7. I am submitting this affidavit in support of a search warrant for a gray covered Coolpad cellular telephone, Model Coolpad 3632A, IMEI number 862429035621539, hereinafter referred to as "Device A." Device A is currently on Milwaukee Police Department Inventory # 18001329 as Item #1 and is currently located at the North Central HIDTA, 801 W. Michigan Street, Milwaukee, WI.

8. I am also submitting this affidavit in support of a search warrant for a silver cased iPhone, Model MQ3X2LL/A, Serial Number F17VPX1DHYFK, IMEI 35 578907 295887 8, hereinafter referred to as "Device B." Device B is currently on Milwaukee Police Department Inventory #18001180 as Item #2 and is currently located at North Central HIDTA, 801 W. Michigan Street, Milwaukee, WI.

9. The applied-for warrant would authorize the forensic examination of Device A and Device B for the purpose of identifying electronically stored data more particularly described in Attachment B.

II. PROBABLE CAUSE

10. I am currently participating in an investigation of a large-scale marijuana drug trafficking organization (“DTO”) led by Josef K. Habib and others. I am familiar with the facts and circumstances regarding this investigation as a result of my personal participation in this investigation via (a) reports prepared by, and information obtained from, other federal, state, and local law enforcement agents and officers, all of whom I believe to be truthful and reliable; and (b) information obtained from cooperating citizen witnesses, confidential sources, and defendants. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

11. In 2017, members of the Milwaukee Police Department initiated an investigation into the drug trafficking activities of Josef K. Habib and other individuals. Habib acquired large shipments of marijuana from out of state source(s) which Habib then distributed in the greater Milwaukee area. Habib was also identified as utilizing stash locations in the greater Milwaukee area, including the Cities of Milwaukee and Greenfield Wisconsin.

12. On January 8, 2018, law enforcement officers conducted surveillance at an identified stash location for Habib, 4100 W. Hillcrest Dr., #207, Greenfield, WI. While conducting surveillance, officers observed a vehicle known to be driven by Habib, a black Nissan Maxima, bearing Wisconsin license 242LWL, parked in a visitor parking stall at 4100 W. Hillcrest Dr., near the garage corresponding to apartment #207. Law enforcement officers observed that the overhead garage door on the attached garage corresponding to apartment 207 was fully open.

13. Shortly thereafter, law enforcement officers observed a Toyota Highlander bearing Virginia license plates arrive and drive into the open garage corresponding to apartment #207. After the vehicle entered the garage, the garage door immediately closed.

14. Approximately 20 minutes later, law enforcement officers observed the overhead garage door open to the garage corresponding to apartment #207. A law enforcement officer observed a white male enter the driver's seat of the Toyota Highlander. At the time, Habib was standing in front of this vehicle. The Toyota Highlander then moved in reverse out of the garage, and once out of the garage drove from the area. Officers then observed Habib enter the Nissan Maxima. Habib then drove it into the garage corresponding to apartment #207. As soon as the vehicle entered the garage, the overhead door closed.

15. Approximately 25 minutes later, the overhead door of the garage corresponding to apartment #207 opened and the Nissan Maxima exited in reverse. Officers observed that Habib was driving the vehicle, and was its sole occupant.

16. Officers conducted a stop of the Nissan Maxima directly outside the address at 4100 W. Hillcrest Drive. Officers conducting the stop of Habib detected an odor of marijuana emanating from the vehicle. In part, officers observed a large black plastic garbage bag located on the rear passenger seat. A complete search of the Nissan Maxima revealed a total of approximately 64 pounds of suspected marijuana within the trunk and rear passenger area of the vehicle. An officer conducted a field test on samples of the marijuana seized from the Maxima, and the suspected marijuana tested positive for the presence of THC, the active ingredient in marijuana. Authorities also seized a **gray covered Coolpad cellular telephone, Model Coolpad 3632A, IMEI number 862429035621539** from the vehicle.

17. Search warrants were subsequently executed on January 8, 2018, at 4100 W. Hillcrest Drive #207, Greenfield Wisconsin, and at the residence of Habib located at 117 W. Walker Street, Apartment #303, Milwaukee, WI.

18. Law enforcement officers recovered approximately 206 pounds of marijuana from 4100 W. Hillcrest Drive #207, Greenfield; and, from 117 W. Walker Street, Apartment #303, Milwaukee, Wisconsin, Habib's residence, approximately 16 pounds of marijuana, in excess of \$21,500 in U.S. currency, a loaded .40 caliber pistol, and a **silver cased iPhone, Model MQ3X2LL/A, Serial Number F17VPX1DHYFK, IMEI 35 578907 295887 8.** Law enforcement authorities also recovered items consistent with the packaging and distribution of controlled substances.

19. During the execution of the search warrant at 117 W. Walker Street, apartment #303, a *Mirandized* interview of Habib's live in girlfriend, Corianne Markowski, occurred. Markowski identified the above-referenced iPhone, Device B, as belonging to Habib.

20. On January 23, 2018, a grand jury sitting in the Eastern District of Wisconsin returned an indictment against Habib alleging money laundering, drug trafficking, and the use of a firearm in furtherance of drug trafficking. This case is identified as *United States v. Habib and Markowski*, Case No. 18-CR-16.

III. TECHNICAL TERMS

21. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. **Wireless telephone:** A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of

transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence

of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.
- f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

22. Based on my training, experience, and research, I know that Devices have the capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA and all have the ability to access the internet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the devices.

IV. ELECTRONIC STORAGE AND FORENSIC ANALYSIS

23. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the

Internet are typically stored for some period of time on the devices. This information can sometimes be recovered with forensics tools.

24. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

25. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of Device A and B consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the devices to human inspection in order to determine whether it is evidence described by the warrant.

26. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

V. CONCLUSION

27. Based on the above information, there is probable cause to believe that Josef K. Habib is involved in (1) money laundering in violation of Title 18, United States Code, Section 1956; (2) the possession of marijuana with the intent to distribute in violation of Title 21, United States Code, Sections 841(a)(1), (b)(1)(B) and (b)(1)(C); and, (3) the possession of a firearm in furtherance of drug trafficking in violation of Title 18 United States Code, Section 924(c). There is also probable cause to search Device A and Device B, which is more particularly described in Attachment A, and which is currently located at North Central HIDTA, Milwaukee, Wisconsin, for evidence of these crimes, as described in Attachment B.

ATTACHMENT A

The property to be searched is:

1. One gray covered Coolpad cellular telephone, Model Coolpad 3632A, IMEI number 862429035621539, Device A. Device A is currently located at North Central HIDTA, 801 W. Michigan Street, Milwaukee, WI. Device A is currently listed under Milwaukee Police Department Inventory # 18001329 as item number 1.
2. A silver cased iPhone, Model MQ3X2LL/A, Serial Number F17VPX1DHYFK, IMEI 35 578907 295887 8, Device B. Device B is currently located at North Central HIDTA, 801 W. Michigan Street, Milwaukee, WI. Device B is currently listed under Milwaukee Police Department Inventory # 18001180 as item number 2.

ATTACHMENT B

1. All records on the Devices described in Attachment A that relate to violations of Title 21, United States Code, Section 841(a)(1), (b)(1)(B), (b)(1)(C), and Title 18, United States Code Section 2 (Knowingly and Intentionally Possessing with the Intent to Deliver a Controlled Substance, Marijuana), Title 18, United States Code, Section 924(c)(1)(A)(i) (Knowingly Possessing a Firearm in Furtherance of Drug Trafficking), and Title 18, United States Code, Section 1956 (Money Laundering), including:

- a. Electronic drug or money ledgers, drug distribution or customer lists and related identifying information, drug supplier lists (including names, addresses, phone numbers, or any other identifying information); correspondence, notations, logs, receipts, journals, books, records, and other documents noting the price, quantity, and/or times when controlled substances were obtained, transferred, sold, distributed, and/or concealed lists of customers and related identifying information; types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions; types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;
- b. Electronic telephone books, address books, telephone bills, photographs, letters, cables, telegrams, facsimiles, personal notes, e-mails, documents, and other items or lists reflecting names, addresses, telephone numbers, addresses, and any communications regarding illegal activities among and between members and associates involved in drug trafficking activities;
- c. Records, items and documents stored on the Devices reflecting travel for the purpose of participating in drug trafficking activities, such as passports, airline tickets, bus tickets, vehicle rental receipts, credit card receipts, taxi cab receipts, hotel and restaurant receipts, canceled checks, maps, and records of long distance calls reflecting travel from August 2012 to the present;
- d. Bank account records, loan documents, wire transfer records, money order receipts, postal express mail envelopes, UPS, FedEx, and other mail service receipts and records, bank statements, checks, credit card records, safe deposit box records, records and receipts and rental agreements for storage facilities, financial records and notes showing payment, receipt, concealment, transfer, or movement of money

generated from the sale of controlled substances, or financial transactions related to the trafficking of controlled substances.

- e. Photographs, videotapes or other depictions of assets, co-conspirators, controlled substances, or other activities related to drug trafficking or money laundering.
- f. Records of Internet Protocol addresses used; records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user typed web addresses.

2. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

3. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.